PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference S0053PCT	**FOR FURTHER ACTION**	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/FI 03/00046	International filing date *(day/month/year)* 21.01.2003	Priority date *(day/month/year)* 22.01.2002
International Patent Classification (IPC) or both national classification and IPC H04L29/06		
Applicant INTRASECURE NETWORKS OY et al.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 6 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 4 sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the opinion
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
   - VI ☐ Certain documents cited
   - VII ☐ Certain defects in the international application
   - VIII ☐ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
21.08.2003	05.05.2004
Name and mailing address of the international preliminary examining authority: European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized Officer Kopp, K Telephone No. +49 89 2399-7833

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/FI 03/00046

I. Basis of the report

1. With regard to the **elements** of the international application *(Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17))*:

Description, Pages

1-13 as originally filed

Claims, Numbers

1-20 filed with telefax on 26.03.2004

Drawings, Sheets

1/2-2/2 as originally filed

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

   These elements were available or furnished to this Authority in the following language: , which is:

   ☐ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).

   ☐ the language of publication of the international application (under Rule 48.3(b)).

   ☐ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

   ☐ contained in the international application in written form.

   ☐ filed together with the international application in computer readable form.

   ☐ furnished subsequently to this Authority in written form.

   ☐ furnished subsequently to this Authority in computer readable form.

   ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

   ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

   ☐ the description, pages:

   ☐ the claims, Nos.:

   ☐ the drawings, sheets:

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)).

   (Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)

6. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-20
	No:	Claims	
Inventive step (IS)	Yes:	Claims	1-20
	No:	Claims	
Industrial applicability (IA)	Yes:	Claims	1-20
	No:	Claims	

2. Citations and explanations

   see separate sheet

Re Item V

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Reference is made to the following documents:

   D1: WO 99/35799
   D2: WO 00/56034

   The document D1 was not cited in the international search report. A copy of the document is appended hereto.

2. The subject-matter of claim 1 is new (Article 33(2) PCT).

   The document D1 is regarded as being the closest prior art to the subject-matter of claim 1 and discloses (the references in parentheses applying to this document):

   - Method for sending messages over secure communication links in networks comprising at least a first terminal being able to change its method of network access and at least one other terminal with one or more possible intermediate computers between the first terminal and the other terminal performing network address and/or other translations (page 2, lines 6-10), a secure communication link being established between an initial network address of the first terminal and the address of the other terminal, the link defining at least the addresses of the two terminals, and performing encapsulation in said secure communication link to overcome network address and/or other translations made by said intermediate computes on the route (page 4, lines 12-16), characterized by

   The subject-matter of claim 1 differs from the disclosure of D1 in that
   - a) the first terminal moving from said initial network address to a new network address,
   - b) sending a request message using encapsulation from the first terminal to the other terminal to change said secure connection to be between the new address of the first terminal and the other terminal, the request also

containing a description of the encapsulation method performed by the first terminal on the basis of which description the other terminal detects translations performed by said intermediate computers,

- c) the other terminal responding to the first terminal with a reply message with a description about translations made by said possible intermediate computers between the new address of the first terminal and the other terminal and/or encapsulation methods supported by the other terminal, and
- d) thereafter sending the message from the first terminal to the other terminal by using the information sent with said reply.

3. The problem to be solved by the present invention may be regarded as source initiated changes of communication parameters to protect from network based attacks like spoofing or data intercepting.

4. The solution to this problem proposed in claim 1 of the present application is considered as involving an inventive step (Article 33(3) PCT).

D1 does not lead in the direction of the subject-matter as claimed in claim 1 for the following reasons: the address translations and/or protocol conversions that are performed on messages between the first terminal and the other terminal are dynamically discovered by exchanging a probe, and comparing information in the probe against its known form at the moment of sending. These changes are compensated when the message authentication code is computed. However, the first terminal does not move from the initial address to a new network address to change the secure connection to be between the new address of the first terminal and the other terminal.

D2 is less relevant, because it discloses a method allowing Internet Protocol security protocol to be used with network address translation, i.e. by mapping multiple local IP address and a Security Parameter Index associated with an inbound IP security protocol Security Association to a global IP address.

None of the cited prior art documents describe the specific execution of the method as claimed in claim 1 to solve the above mentioned problem. All these documents show different realisations of how to overcome network address translations made by intermediate computers on the route of messages sent over

secure communications links.

The person skilled in the art would not obviously derive the claims solution from D1, or from D1 in combination with D2.

5. Claims 2-20 are dependent on claim 1 and as such also meet the requirements of the PCT with respect to novelty and inventive step.

6. Remark on claim 5: the wording "step c)" should apparently be read "step b)".

CLAIMS

1. Method for sending messages over secure communication links in networks comprising at least one mobile terminal and at least one other terminal with one or more possible intermediate computers between the mobile terminal and the other terminal performing network address and/or other translations, the secure communication link being established between an initial network address of the mobile terminal and the address of the other terminal,
   characterized by
   a) establishing a secure communication link between an initial address of the mobile terminal and the address of the other terminal, the link defining at least the addresses of the two terminals and supporting some method to overcome network address and/or other translations made by intermediate computers on the route,
   b) the mobile terminal moving from an initial network address to a new network address,
   c) sending a request message using the method of step a) from the mobile terminal to the other terminal to change the secure connection to be between the new address of the mobile terminal and the other terminal, the request also containing a description of the overcoming method performed by the mobile terminal and/or other information that enables the other terminal to detect translations performed by the intermediate computers,
   d) the other terminal responding to the mobile terminal with a reply message with a description about translations made by possible intermediate computers between the new address of the mobile terminal and the other terminal and/or encapsulation methods supported by the other terminal, and
   e) thereafter sending the message from the mobile terminal to the other terminal by using the information sent with said reply.

2. Method of claim 1, characterized in that, the description of the message include source and/or destination addresses that enables the receiving terminal to detect address translations performed by intermediate computers.

3. Method of claim 1, c h a r a c t e r i z e d in that the description of the message includes information about encapsulation protocols, as well as source and destination TCP or UDP ports.

4. Method of claim 3, c h a r a c t e r i z e d in that the NAT traversal is performed by UDP encapsulation, TCP encapsulation and/or by some other encapsulation.

5. Method of any of claims 1 - 4, c h a r a c t e r i z e d in that after receiving of the request message by said other terminal sent in step c), the other terminal determines by examining the request, which translations and/or encapsulations are required in the traffic between the mobile terminal and the other terminal.

6. Method of claim 5, c h a r a c t e r i z e d in that the reply message of step d) contains information about the communication link to be used between the new address of the mobile terminal and said other terminal.

7. Method of claim 6, c h a r a c t e r i z e d in that the information about the communication link includes information about whether NAT traversal and/or other encapsulation should be used.

8. Method of any of claims 1 - 5, c h a r a c t e r i z e d in that in step d) the mobile terminal compares the descriptions of the request respective reply messages and sends all subsequent messages from this new network address on the basis of the comparison telling what encapsulations, protocols and rules should be used in the further communication.

9. Method of any of claims 1 - 8, c h a r a c t e r i z e d in that the secure communication link is formed by using the IPSec protocol.

10. Method of claim 9, c h a r a c t e r i z e d in that the message in step e) is sent by using IPSec and NAT traversal updated to the new network address of the mobile terminal.

11. Method of any of claims 1 - 8, c h a r a c t e r i z e d in that the message in step e) is sent without NAT traversal or other changes in the communication link if on the basis of the comparison in claim 8, the descriptions correspond to each other or if so informed by the other terminal in claim 7.

12. Method of any of claims 1 -11, c h a r a c t e r i z e d in that the secure connection is an IPSec SA.

13. Method of claim 12, c h a r a c t e r i z e d in that for forming the IPSec SA, a key exchange mechanism that passes through NAT is used.

14. Method of claim 12, c h a r a c t e r i z e d in that the key exchange protocol is IKE if the NAT device supports the UDP protocol.

15. Method of claim 14, c h a r a c t e r i z e d in that for forming the IPSec SA, a key exchange mechanism is used wherein several traversal mechanisms are used simultaneously to increase the chance that at least one of them pass through the NAT device.

16. Method of claim 12, c h a r a c t e r i z e d in that for forming the IPSec SA, a key exchange mechanism is performed in which a negotiation process is used to agree on protocols to be used in the further communication.

17. Method of claim 12, c h a r a c t e r i z e d in that for forming the IPSec SA, the most common encapsulation protocol is used in the key exchange mechanism.

18. Method of any of claims 1 - 17, c h a r a c t e r i z e d in that the address of the other terminal is the end destination address of messages sent from the mobile terminal, in which case transport or tunnel mode is used in the IPSec communication.

19. Method of any of claims 1 - 17, c h a r a c t e r i z e d in that the destination address of the message is the address of a host which is not the other terminal, in which case tunnel mode or transport mode together with a tunnelling protocol is used in the IPSec communication.

20. Method of any of claims 1 - 7, 9 - 19, c h a r a c t e r i z e d in that several request messages of step c) are sent, each processed using a different traversal mechanism, where after the other terminal indicates in the reply which methods is to be used in the further communication.